

WHAT IS CLAIMED IS:

1 1. An apparatus for providing a secure universal
2 serial bus (USB) comprising a secure channel for
3 transferring data.

1 2. An apparatus as claimed in Claim 1 wherein said
2 apparatus comprises a secure USB domain device coupled to
3 an external host computer.

1 3. An apparatus as claimed in Claim 2 wherein said
2 secure USB domain device comprises:

3 a USB memory device that is not accessible by said
4 host computer;

5 a USB processor that is not accessible by said host
6 computer;

7 a USB host controller that is not accessible by said
8 host computer; and

9 an internal USB bus that couples said USB memory
10 device, said USB processor, and said USB host controller.

1 4. An apparatus as claimed in Claim 3 further
2 comprising a USB node coupled to said USB bus, said USB
3 node capable of being coupled to a USB tree.

1 5. An apparatus as claimed in Claim 1 wherein said
2 apparatus comprises a secure USB domain device embedded
3 within a host computer.

1 6. An apparatus as claimed in Claim 5 wherein said
2 secure USB domain device comprises:

3 a USB memory device that is not accessible by said
4 host computer;

5 a USB processor that is not accessible by said host
6 computer;

7 a USB host controller that is not accessible by said
8 host computer; and

9 an internal USB bus that couples said USB memory
10 device, said USB processor, and said USB host controller.

1 7. An apparatus as claimed in Claim 6 further
2 comprising a virtual conduit interface coupled to said
3 secure USB domain device and coupled to at least one non-USB
4 device, said virtual conduit interface capable of providing
5 a secure USB channel for transferring information to said at
6 least one non-USB device.

1 8. An apparatus for providing a secure universal
2 serial bus (USB) capable of transferring information over a
3 secure channel to and from a device coupled to a host
4 computer, wherein said host computer is coupled to other
5 host computers in a data network, said apparatus comprising:

6 at least one host computer capable of supporting USB
7 input/output devices, said at least one host computer
8 comprising a USB bus, USB client software, and USB System
9 software; and

10 a secure USB domain device capable of one of: blocking
11 outgoing data flows of confidential information, forwarding
12 outgoing data flows of encrypted confidential information,
13 and forwarding outgoing data flows of non-confidential
14 information.

1 9. The apparatus as claimed in Claim 8 wherein said
2 secure USB domain device comprises:

3 a plurality of USB devices;

4 a first set of data channels for exchanging data with
5 each of said plurality of USB devices; and

6 a second set of data channels for exchanging data
7 between said secure USB domain device and said at least one
8 host computer.

1 10. An apparatus as claimed in Claim 8 wherein said
2 secure USB domain device is embedded within said at least
3 one host computer.

1 11. An apparatus as claimed in Claim 10 wherein said
2 secure USB domain device comprises:

3 a USB bus;

4 a memory coupled to said USB bus capable of storing
5 each data packet sent from, or received by, said secure USB
6 domain device, said memory containing a set of buffers,
7 each of said buffers comprises data associated with said
8 Host or to said device;

9 circuitry coupled to said USB bus, said circuitry
10 capable of forwarding commands and requests for information

11 received in said secure USB domain device to corresponding
12 devices;

13 a processor coupled to said USB bus, said processor
14 capable of one of: classifying data packets, controlling
15 forwarding operations, and controlling encryption
16 operations; and

17 a USB host controller coupled to said USB bus, said
18 USB host controller capable of managing data flow between
19 said at least one host computer and a plurality of USB
20 devices.

1 12. An apparatus as claimed in Claim 11 wherein said
2 apparatus further comprises a virtual conduit interface
3 coupled to said secure USB domain device and coupled to at
4 least one non-USB device, said virtual conduit interface
5 capable of providing a secure USB channel for transferring
6 information to said at least one non-USB device.

1 13. An apparatus as claimed in Claim 8 wherein said
2 secure USB domain device is coupled to said at least one
3 external host computer.

1 14. An apparatus as claimed in Claim 13 wherein said
2 secure USB domain device comprises:

3 a USB bus;

4 a memory coupled to said USB bus capable of storing
5 each data packet sent from, or received by, said secure USB
6 domain device, said memory containing a set of buffers,
7 each of said buffers comprises data associated with said
8 Host or to said device;

9 circuitry coupled to said USB bus, said circuitry
10 capable of forwarding commands and requests for information
11 received in said secure USB domain device to corresponding
12 devices;

13 a processor coupled to said USB bus, said processor
14 capable of one of: classifying data packets, controlling
15 forwarding operations, and controlling encryption
16 operations; and

17 a USB host controller coupled to said USB bus, said
18 USB host controller capable of managing data flow between
19 said at least one host computer and a plurality of USB
20 devices.

1 15. A method for providing a secure universal serial
2 bus (USB) capable of transferring information over a secure
3 channel to and from a device coupled to a host computer,
4 wherein said host computer is coupled to other host
5 computers in a data network, said method comprising the
6 steps of:

7 providing at least one host computer capable of
8 supporting USB input/output devices, said at least one host
9 computer comprising a USB Bus, USB client software, and USB
10 System software; and

11 providing a secure USB domain device capable of one
12 of: blocking outgoing data flows of confidential
13 information, forwarding outgoing data flows of encrypted
14 confidential information, and forwarding outgoing data
15 flows of non-confidential information.

1 16. The method as claimed in Claim 15 wherein the
2 step of providing a secure USB domain device capable of one
3 of: blocking outgoing data flows of confidential
4 information, forwarding outgoing data flows of encrypted
5 confidential information, and forwarding outgoing data
6 flows of non-confidential information, comprises the steps
7 of:

8 storing each data packet received by said secure USB
9 domain device in a memory containing a set of buffers, each
10 of said buffers comprising data associated with one of:
11 said at least one host computer, and said device coupled to
12 said at least one host computer;

13 forwarding commands and requests for information
14 received in said secure USB domain device to a
15 corresponding device;

16 classifying each data packet sent from said device to
17 said secure USB domain device to one of: a first data type
18 that requires no intervention, and a second data type that
19 requires intervention according to a buffer association;

20 forwarding data packets of the first type that are
21 originated at said device to said at least one host
22 computer;

23 blocking data packets of the second type that contain
24 confidential information;
25 forwarding data packets of the second type that
26 contain encrypted confidential information; and
27 forcing any exchange of data between said at least one
28 host computer and said device to flow through said secure
29 USB domain device.

1 17. The method as claimed in claim 16, wherein the
2 step of blocking data packets of the second type that
3 contain confidential information, and the step of
4 forwarding data packets of the second type that contain
5 encrypted confidential information, comprise the steps of:
6 interrogating a header of each data packet of the
7 second type to reveal the type of information required from
8 a device;
9 transferring said information in an encrypted form if
10 the information is required at another host computer for
11 further actions;
12 performing the following steps if said information is
13 required for data verification:
14 blocking the data packet;
15 receiving verification information from said host
16 computer in an encrypted form;

17 decrypting said verification information;
18 comparing said encrypted verification information with
19 information received from said device; and
20 providing said host computer with an indication
21 verifying whether a match was detected.

1 18. The method as claimed in Claim 15, wherein secure
2 information is transferred between said host computer and
3 said secure USB domain device in a enciphered form, thereby
4 establishing at least one secure data channel between said
5 host computer and said secure USB domain device.

1 19. The method as claimed in Claim 15, wherein data
2 flows from a first device to a second device directly
3 through said secure USB domain device without utilizing
4 resources of said host computer.

1 20. The method as claimed in Claim 15, further
2 comprising the steps of:
3 coupling a virtual conduit interface to said secure
4 USB domain device;
5 coupling said virtual conduit interface to at least
6 one non-USB device; and
7 using said virtual conduit interface to provide a
8 secure USB channel for transferring information to said at
9 least one non-USB device.